IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of: **FOX ET AL.**	)	
	)	Examiner: K. Abrishamkar
Serial No. **09/500,108**	)	
Filing Date: **February 8, 2000**	)	
Confirmation No. **2137**	)	Art Unit: 2131
For: **SYSTEM AND METHOD FOR ASSESSING THE SECURITY POSTURE OF A NETWORK**	)	

SUPPLEMENTAL DECLARATION UNDER 37 CFR §1.131

Mail Stop Amendment
Commissioner for Patents
P. O. Box 1450
Alexandria, VA 22313-1450

Sir:

We, **KEVIN L. FOX, RONDA R. HENNING, JOHN T. FARRELL and CLIFFORD C. MILLER**, do hereby declare and state:

1. We are the co-inventors of claims 1-36 as originally filed in the above-identified patent application.

2. We conceived the subject matter of the above-identified patent application while working in our laboratories in the United States at Harris Corporation in Palm Bay, Florida

prior to December 29, 1998, the effective date of U.S. Patent No. 6,415,321 to Gleichauf et al.

3. This Supplemental Declaration is filed in response to the Office Action mailed May 4, 2004, in which the Examiner stated there was not sufficient evidence on the exhibits (1-6) supplied by the Applicants to demonstrate that our work was completed before the filing date of the Gleichauf reference. For example, the Examiner noted that Exhibits 1-6 should have a date of publication associated with them.

4. Applicants resubmit in this Supplemental Declaration the same Exhibits 1-6 with associated dates. For example, Exhibit 1 now includes the unredacted date of October 6, 1998. Exhibits 2 and 3 did not have dates printed on them, but were stored electronically with the associated date of about December 19, 1998. Exhibit 4 was stored electronically with the associated date of February 1, 1999. Exhibit 5 includes the unredacted date of March 11, 1999. Exhibit 6 was stored electronically and has an associated date of March 23, 1999.

5. Applicants have located other evidence that conclusively shows that we conceived and reduced to practice the claimed invention before December 29, 1998. Applicants submit

new Exhibit 01, which is dated September 25, 1998. New Exhibit 1A is dated November 1998. New Exhibit 3A is dated January 1999.

6. We conceived and reduced to practice before December 29, 1998 a method, computer program and data processing system for accessing the security posture of a network that creates a system object model database representing a network and supports the information data requirements of disparate network vulnerability analysis programs. The system object model database is exported to the programs. The network is analyzed with each program to produce data results, which are correlated to determine the security posture of the network.

7. From the time of conception, we worked diligently to complete the invention before December 29, 1998. After reducing to practice the invention as claimed before December 29, 1998, we worked to improve the invention software, including the layout of the graphical user interface, and filed a patent application on our invention.

8. Exhibit 01 dated September 25, 1998 clearly shows that we had developed core concepts for the NVT architecture. It uses different tool inputs, for example, network vulnerability analysis programs. The system creates a database that represents

the network and uses various engines that are selected concerning the disparate network vulnerability/risk analysis programs. Data is combined/correlated to reach a unified report as a simple answer.

9. Exhibit 1, dated October 6, 1998, is a task report for the network visualization tool (NVT). This document shows that the complete conception had occurred and we were working towards reduction to practice of the present invention, including the creation of a database as a system object model to support data requirements of disparate network vulnerability analysis programs. These would be exported and the network analyzed and data results correlated.

10. Exhibit 1A is dated November 1998, before the effective date of December 29, 1999, and clearly shows that we had begun to develop the detailed software for the network vulnerability system that assesses the security posture of a network as claimed. For example, the first part of the exhibit under the title of Architecture Concept shows different core components of data storage and the use of plug-ins for autonomous tools of problem domain specific applications. The analysis flow diagram shows that there can be manual or automatic input for

system description data and different results imported from risk assessment tools corresponding to the different analysis programs. Data fusion and description data validation can occur to determine inconsistencies. Any required data can be exported to the risk assessment tools. In Exhibit 1A, the slides that are titled Neural Network/Learning Systems, Fuzzy Logic Systems, and Fuzzy Technologies, show an example of correlation used in the present invention. An example of a software program used by us when reducing to practice the invention was FuzzyCLIPS. Examples of the software logic are in the CLIPS and FuzzyCLIPS section. The section entitled, "CLIPS-Rules" and the following slides show that software logic was already developed by the time Exhibit 1A was printed in November 1998. Also, the pages titled "FuzzyCLIPS Concepts" sets forth the logic that was used in the software. The section titled Task No. 6 shows a proof-of-concept prototype that had been developed. Those slides describe simple working examples, for example, the testing by using an internet scanner, ANSSR and RAM. The graphical user interface was developed at this time (before December 29, 1998) and is described in Exhibit 1A at sections titled Automatic Discovery Manual, Network Diagram, and Network Node Evaluation. These slides show that we

had reduced to practice the broad concept of the invention by November 1998, before the effective December 29, 1998 date.

11. Exhibit 2 was also produced before December 29, 1998. It is a short abstract by two co-inventors of the present invention. This abstract explains how the inventors through their corporate entity had been conducting research for a single topological model to support multiple vulnerability analysis tools and the notes beginning of prototype development again emphasizing the reduction to practice of the claimed invention. Exhibit 3 was also produced before December 29, 1998, and sets forth different prototype design notes emphasizing again the reduction to practice.

12. Exhibit 3A are notes of a Technical Interchange Meeting just after the effective date of Gleichauf. This exhibit shows further development, for example, clearly shows the design enhancements in the graphical user interface and node representation. It shows further software development as set forth by the logic diagrams and prototype architecture.

13. Later development was completed and included enhancements to the architecture as shown in Exhibit 4, showing fuzzy fusion as operative with the system object model. Exhibit

5 is similar to Exhibit 4 and shows the fuzzy fusion process in greater detail. Exhibit 6 is a white paper describing a brief overview of the system vulnerability analysis with the network visualization tool of the present invention.

14. The exhibits set forth in this Supplemental Declaration conclusively show that not only had we conceived the claimed invention prior to December 29, 1998, the effective date of U.S. Patent No. 6,415,321 to Gleichauf, et al., but also we had reduced to practice the invention as noted by the logic examples, software examples, and the graphical user interface slides of Exhibit 1A, including other logic diagrams for the fuzzy logic and/or fusion that would be used for correlating data results of the network vulnerability analysis programs and determining the security posture of the network.

15. We hereby declare that all statements made herein of our own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may

jeopardize the validity of the application or any patent issued thereon.

7/22/04
Date

KEVIN L. FOX

7/22/04
Date

RONDA R. HENNING

7/22/2004
Date

JOHN T. FARRELL

7/22/04
Date

CLIFFORD C. MILLER